

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

Commissioner
 US Department of Commerce
 United States Patent and Trademark
 Office, PCT
 2011 South Clark Place Room
 CP2/5C24
 Arlington, VA 22202
 ETATS-UNIS D'AMERIQUE
 en sa qualité d'office élu

Date d'expédition (jour/mois/année) 12 juin 2001 (12.06.01)	
Demande internationale no PCT/IB00/01157	Référence du dossier du déposant ou du mandataire B-14-312-PCT
Date du dépôt international (jour/mois/année) 24 août 2000 (24.08.00)	Date de priorité (jour/mois/année) 30 août 1999 (30.08.99)
Déposant SASSELLI, Marco etc	

1. L'office désigné est avisé de son élection qui a été faite:

☒ dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

17 mars 2001 (17.03.01)

☐ dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection ☒ a été faite
☐ n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse no de télécopieur: (41-22) 740.14.35	Fonctionnaire autorisé Pascal Piriou no de téléphone: (41-22) 338.83.38
--	---

This Page Blank (uspto)

TRAITE D'COOPERATION EN MATIERE DE BREVETS

PCT

NOTIFICATION DE L'ENREGISTREMENT
D'UN CHANGEMENT(règle 92bis.1 et
instruction administrative 422 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

WENGER, Joel
Leman Consulting S.A.
62 route de Clementy
CH-1260 Nyon
SUISSE

Date d'expédition (jour/mois/année) 17 juillet 2001 (17.07.01)	NOTIFICATION IMPORTANTE
Référence du dossier du déposant ou du mandataire P-14-312-PCT	
Demande internationale no PCT/IB00/01157	Date du dépôt international (jour/mois/année) 24 août 2000 (24.08.00)

1. Les renseignements suivants étaient enregistrés en ce qui concerne:	
<input type="checkbox"/> le déposant	<input type="checkbox"/> l'inventeur <input checked="" type="checkbox"/> le mandataire <input type="checkbox"/> le représentant commun
Nom et adresse WENGER, Joel Griffes Consulting S.A. 81, route de Florissant CH-1206 Genève SUISSE	Nationalité (nom de l'Etat) Domicile (nom de l'Etat)
	no de téléphone 41 22 346 33 93
	no de télécopieur 41 22 347 30 11
	no de tél'imprimeur
2. Le Bureau international notifie au déposant que le changement indiqué ci-après a été enregistré en ce qui concerne:	
<input type="checkbox"/> la personne <input type="checkbox"/> le nom <input checked="" type="checkbox"/> l'adresse <input type="checkbox"/> la nationalité <input type="checkbox"/> le domicile	
Nom et adresse WENGER, Joel Leman Consulting S.A. 62 route de Clementy CH-1260 Nyon SUISSE	Nationalité (nom de l'Etat) Domicile (nom de l'Etat)
	no de téléphone 41 22 363 78 78
	no de télécopieur 41 22 363 78 70
	no de tél'imprimeur
3. Observations complémentaires, le cas échéant:	
4. Une copie de cette notification a été envoyée:	
<input checked="" type="checkbox"/> à l'office récepteur	<input type="checkbox"/> aux offices désignés concernés
<input type="checkbox"/> à l'administration chargée de la recherche internationale	<input checked="" type="checkbox"/> aux offices élus concernés
<input checked="" type="checkbox"/> à l'administration chargée de l'examen préliminaire international	<input type="checkbox"/> autre destinataire:

Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse no de télécopieur (41-22) 740.14.35	Fonctionnaire autorisé: R. Chrem no de téléphone (41-22) 338.83.38
---	--

This Page Blank (uspto)

CORRECTED
VERSION

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

NOTIFICATION DE L'ENREGISTREMENT
D'UN CHANGEMENT(règle 92bis.1 et
instruction administrative 422 du PCT)

Destinataire:

LEMAN CONSULTING S.A.
62 route de Clementy
CH-1260 Nyon
SUISSE

Date d'expédition (jour/mois/année) 21 septembre 2001 (21.09.01)	NOTIFICATION IMPORTANTE
Référence du dossier du déposant ou du mandataire P-14-312-PCT	
Demande internationale no PCT/IB00/01157	Date du dépôt international (jour/mois/année) 24 août 2000 (24.08.00)

1. Les renseignements suivants étaient enregistrés en ce qui concerne:									
<input type="checkbox"/> le déposant	<input type="checkbox"/> l'inventeur								
<input checked="" type="checkbox"/> le mandataire	<input type="checkbox"/> le représentant commun								
Nom et adresse WENGER, Joel Leman Consulting S.A. 62 route de Clementy CH-1260 Nyon SUISSE	<table border="1"> <tr> <td>Nationalité (nom de l'Etat)</td> <td>Domicile (nom de l'Etat)</td> </tr> <tr> <td colspan="2">no de téléphone 41 22 346 33 93</td> </tr> <tr> <td colspan="2">no de télécopieur 41 22 347 30 11</td> </tr> <tr> <td colspan="2">no de téléimprimeur</td> </tr> </table>	Nationalité (nom de l'Etat)	Domicile (nom de l'Etat)	no de téléphone 41 22 346 33 93		no de télécopieur 41 22 347 30 11		no de téléimprimeur	
Nationalité (nom de l'Etat)	Domicile (nom de l'Etat)								
no de téléphone 41 22 346 33 93									
no de télécopieur 41 22 347 30 11									
no de téléimprimeur									
2. Le Bureau international notifie au déposant que le changement indiqué ci-après a été enregistré en ce qui concerne:									
<input checked="" type="checkbox"/> la personne	<input type="checkbox"/> le nom								
<input type="checkbox"/> l'adresse	<input type="checkbox"/> la nationalité								
<input type="checkbox"/> le domicile									
Nom et adresse LEMAN CONSULTING S.A. 62 route de Clementy CH-1260 Nyon SUISSE	<table border="1"> <tr> <td>Nationalité (nom de l'Etat)</td> <td>Domicile (nom de l'Etat)</td> </tr> <tr> <td colspan="2">no de téléphone 41 22 363 78 78</td> </tr> <tr> <td colspan="2">no de télécopieur 41 22 363 78 70</td> </tr> <tr> <td colspan="2">no de téléimprimeur</td> </tr> </table>	Nationalité (nom de l'Etat)	Domicile (nom de l'Etat)	no de téléphone 41 22 363 78 78		no de télécopieur 41 22 363 78 70		no de téléimprimeur	
Nationalité (nom de l'Etat)	Domicile (nom de l'Etat)								
no de téléphone 41 22 363 78 78									
no de télécopieur 41 22 363 78 70									
no de téléimprimeur									
3. Observations complémentaires, le cas échéant:									
4. Une copie de cette notification a été envoyée:									
<input checked="" type="checkbox"/> à l'office récepteur	<input type="checkbox"/> aux offices désignés concernés								
<input type="checkbox"/> à l'administration chargée de la recherche internationale	<input checked="" type="checkbox"/> aux offices élus concernés								
<input checked="" type="checkbox"/> à l'administration chargée de l'examen préliminaire international	<input type="checkbox"/> autre destinataire:								

<p>Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse</p> <p>no de télécopieur (41-22) 740.14.35</p>	<p>Fonctionnaire autorisé:</p> <p>R. Chrem</p> <p>no de téléphone (41-22) 338.83.38</p>
--	---

This Page Blank (uspto)

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

REC'D 11 DEC 2001

WIPO PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)



Référence du dossier du déposant ou du mandataire B-14-312-PCT	POUR SUITE A DONNER voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/IB00/01157	Date du dépôt international (jour/mois/année) 24/08/2000	Date de priorité (jour/mois/année) 30/08/1999
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/00		
Déposant NAGRACARD SA et al.		

- Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.
- Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.
 - ☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

Ces annexes comprennent feuilles.

- Le présent rapport contient des indications relatives aux points suivants:

- I ☒ Base du rapport
- II ☐ Priorité
- III ☐ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- IV ☐ Absence d'unité de l'invention
- V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- VI ☐ Certains documents cités
- VII ☒ Irrégularités dans la demande internationale
- VIII ☒ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 17/03/2001	Date d'achèvement du présent rapport 07.12.2001
Nom et adresse postale de l'administration chargée de l'examen préliminaire international:  Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Cretaine, P N° de téléphone +49 89 2399 8828 

This Page Blank (uspto)

I. Base du rapport

1. En ce qui concerne les **éléments** de la demande internationale (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées dans le présent rapport comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)*):

Description, pages:

1-9 version initiale

Revendications, N°:

1-10 version initiale

Dessins, feuilles:

1/2-2/2 version initiale

2. En ce qui concerne la **langue**, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point.

Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: , qui est :

- ☐ la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)).
- ☐ la langue de publication de la demande internationale (selon la règle 48.3(b)).
- ☐ la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3).

3. En ce qui concerne les **séquences de nucléotides ou d'acide aminés** divulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences :

- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposé avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listage des séquences Présenté par écrit, a été fournie.

4. Les modifications ont entraîné l'annulation :

This Page Blank (uspto)

RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale n° PCT/IB00/01157

- ☐ de la description, pages :
- ☐ des revendications, n°s :
- ☐ des dessins, feuilles :

5. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport)

6. Observations complémentaires, le cas échéant :

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui : Revendications 1-10
	Non : Revendications
Activité inventive	Oui : Revendications 1-10
	Non : Revendications
Possibilité d'application industrielle	Oui : Revendications 1-10
	Non : Revendications

2. Citations et explications voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :
voir feuille séparée

VIII. Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :
voir feuille séparée

This Page Blank (uspto)

Concernant le point V**Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration**

L'invention concerne une méthode de cryptage et de décryptage utilisant plusieurs modules d'encryptage-décryptage en série.

Etat de la technique:

US-A-5 594 797 décrit un tel système, dans lequel trois modules d'encryptage sont chaînés, un module en aval traitant les données encryptées par un module en amont après traitement complet effectué par ce dernier.

Problème:

Les techniques d'attaque les plus récentes de type Differential Power Analysis permettent d'attaquer chaque module séparément en établissant les conditions d'entrée ou de sortie de chaque module et en estimant la présence de 1 ou 0 dans une position donnée de la clé de chiffrement de chaque module.

Invention:

Conformément aux caractéristiques de la revendication 1, un module intermédiaire ne démarre pas ses calculs lorsque le résultat du module en amont a terminé mais débute dès qu'une partie seulement des informations sont disponibles pour être traitées. Il n'est ainsi pas possible pour un observateur extérieur d'établir les conditions d'entrée/sortie d'un module puisque les données de sorties d'un module ne sont plus disponibles dans leur ensemble.

Aucun des autres documents cités dans le rapport de recherche ne divulgue ou suggère une telle procédure d'imbrication partielle des calculs de différents modules d'encryptage en cascade. La revendication 1 remplit donc les conditions de l'article 33 PCT. Les revendications 2 à 10 dépendent de la revendication 1 et satisfont donc également, en tant que telles, aux conditions requises par le PCT en ce qui concerne la nouveauté et l'activité inventive.

This Page Blank (uspto)

Concernant le point VII**Irrégularités dans la demande internationale**

Contrairement à ce qu'exige la règle 5.1 a) ii) PCT, la description n'indique pas l'état de la technique antérieure pertinent exposé dans le document US-A-5 594 797 et ne cite pas ce document.

Concernant le point VIII**Observations relatives à la demande internationale**

L'unique revendication indépendante 1 ne remplit les conditions de l'article 6 PCT relatives à la clarté pour les raisons suivantes:

- le terme "le module ... en aval" est ambigu car il peut désigner soit le dernier module de la pluralité de modules en série soit, en accord avec la description, chaque module intermédiaire à partir du deuxième et le dernier module de la série de modules.
- l'expression "débuté son opération dès qu'une partie du résultat...est disponible" n'est pas claire car elle ne précise pas que, conformément à la description, chaque module aval commence à traiter des **données disponibles issues** de son module amont avant que ce dernier n'ait entièrement achevé ses calculs.

This Page Blank (uspto)

101.069714
Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P-14-312-PCT	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/IB00/01157	International filing date (day/month/year) 24 August 2000 (24.08.00)	Priority date (day/month/year) 30 August 1999 (30.08.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/00		
Applicant NAGRACARD SA		

- This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
- This REPORT consists of a total of 5 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).
 These annexes consist of a total of _____ sheets.
- This report contains indications relating to the following items:
 - I ☒ Basis of the report
 - II ☐ Priority
 - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
 - IV ☐ Lack of unity of invention
 - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
 - VI ☐ Certain documents cited
 - VII ☒ Certain defects in the international application
 - VIII ☒ Certain observations on the international application

Date of submission of the demand 17 March 2001 (17.03.01)	Date of completion of this report 07 December 2001 (07.12.2001)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

This Page Blank (uspto)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/IB00/01157

I. Basis of the report

1. With regard to the elements of the international application:*

- ☐ the international application as originally filed
- ☒ the description:
pages _____ 1-9 _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☒ the claims:
pages _____ 1-10 _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☒ the drawings:
pages _____ 1/2-2/2 _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____
- ☐ the sequence listing part of the description:
pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

This Page Blank (uspto)

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**1. Statement**

Novelty (N)	Claims	1-10	YES
	Claims		NO
Inventive step (IS)	Claims	1-10	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-10	YES
	Claims		NO

2. Citations and explanations

The invention relates to an encryption and decryption method using a plurality of encryption-decryption modules in a series.

Prior art:

US-A-5 594 797 describes such a system, wherein three encryption modules are chained; a downstream module processes the data encrypted by an upstream module after the upstream module has completed the processing.

Problem:

The most recent Differential Power Analysis attack techniques enable each module to be attacked separately by establishing the input or output conditions of each module and by estimating the presence of 1 or 0 in a given position of the encryption key of each module.

Invention:

In accordance with the features of Claim 1, an intermediate module does not begin calculating when the result of the upstream module is completed, but begins as

This Page Blank (uspto)

soon as only a portion of the information is available to be processed. Therefore, it is not possible for an outside observer to establish the input/output conditions of a module since output data of a module is not available as a whole.

None of the other documents cited in the search report discloses or suggests such a method of partially interleaving the calculations of different cascade encryption modules. Claim 1 therefore meets the requirements of PCT Article 33. Claims 2 to 10 are dependent on Claim 1 and therefore also meet, as such, the PCT requirements of novelty and inventive step.

This Page Blank (uspto)

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

Contrary to the requirements of PCT Rule 5.1(a)(ii), the relevant prior art disclosed in document US-A-5 594 797 has not been indicated in the description, nor has this document been cited.

This Page Blank (uspto)

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

Independent Claim 1, which is the only independent claim, does not meet the clarity requirements of PCT Article 6, for the reasons discussed below.

- The term "the downstream ... module" is ambiguous since it can refer to either the last module of the plurality of modules in series or, in accordance with the description, each intermediate module starting with the second and the last module in the series of modules.

- The phrase "begins its operation as soon as a portion of the result ... is available" is not clear, since it does not specify that each downstream module begins processing **available data generated** from the upstream module before said upstream module has entirely finished its calculations, as stated in the description.

This Page Blank (uspto)

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire B-14-312-PCT	POUR SUITE voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après A DONNER	
Demande internationale n° PCT/IB 00/ 01157	Date du dépôt international(jour/mois/année) 24/08/2000	(Date de priorité (la plus ancienne) (jour/mois/année) 30/08/1999
Déposant NAGRACARD SA et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

☒ Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. Base du rapport

- a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.
- ☐ la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.
- b. En ce qui concerne les **séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :
- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposée avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. ☐ Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).

3. ☐ Il y a absence d'unité de l'invention (voir le cadre II).

4. En ce qui concerne le titre,

- ☒ le texte est approuvé tel qu'il a été remis par le déposant.
- ☐ Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'abrégé,

- ☒ le texte est approuvé tel qu'il a été remis par le déposant
- ☐ le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure des dessins à publier avec l'abrégé est la Figure n°

- ☒ suggérée par le déposant.
- ☐ parce que le déposant n'a pas suggéré de figure.
- ☐ parce que cette figure caractérise mieux l'invention.

1

☐ Aucune des figures n'est à publier.

This Page Blank (uspto)

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
8 mars 2001 (08.03.2001)

PCT

(10) Numéro de publication internationale
WO 01/17159 A1

(51) Classification internationale des brevets⁷: H04L 9/00

Michael, John [CH/CH]; 10, route de Commugny,
CH-1296 Coppet (CH).

(21) Numéro de la demande internationale: PCT/IB00/01157

(22) Date de dépôt international: 24 août 2000 (24.08.2000)

(74) Mandataire: WENGER, Joel; Griffes Consulting S.A.,
81, route de Florissant, CH-1206 Genève (CH).

(25) Langue de dépôt: français

(81) États désignés (national): AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE,
DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU,
ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS,
LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO,
NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR,
TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(26) Langue de publication: français

(30) Données relatives à la priorité:

1573/99 30 août 1999 (30.08.1999) CH
60/194,171 3 avril 2000 (03.04.2000) US

(71) Déposant (pour tous les États désignés sauf US): NA-
GRACARD SA [CH/CH]; 22, route de Genève, CH-1033
Cheseaux-sur-Lausanne (CH).

(84) États désignés (régional): brevet ARIPO (GH, GM, KE,
LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien
(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen
(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU,
MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM,
GA, GN, GW, ML, MR, NE, SN, TD, TG).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement): SASSELLI,
Marco [CH/CH]; 20, chemin des Roches, CH-1803
Chardonne (CH). NICOLAS, Christophe [CH/CH]; 29,
rue de Lausanne, CH-1028 Préverenges (CH). HILL,

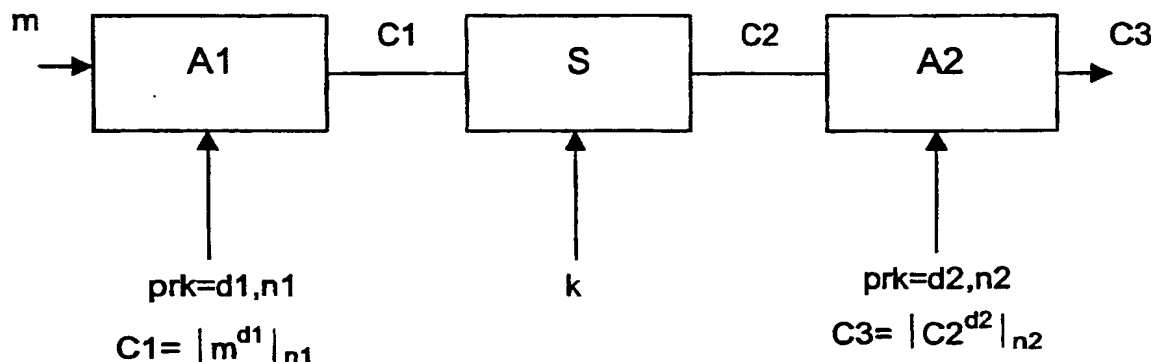
Publiée:

— Avec rapport de recherche internationale.

[Suite sur la page suivante]

(54) Title: MULTIPLE MODULE ENCRYPTION METHOD

(54) Titre: METHODE D'ENCRYPTAGE MULTI-MODULES



(57) Abstract: When an encrypting-decrypting module is being used, there are various methods for determining the key or keys used by said module by analysing the module input or output data. To remedy this inconvenience, the inventive multiple module method is characterised in that the downstream module starts its encrypting-decrypting operations as soon as part of the results of the upstream module is available.

(57) Abrégé: Lors de l'utilisation d'un module d'encryptage-décryptage, des méthodes existent pour déterminer la ou les clés utilisées par le module en analysant les données entrantes ou sortantes du module. Pour pallier ce défaut, la méthode multi-modules proposée consiste à ce que le module aval débute ses opérations d'encryptage-décryptage dès qu'une partie des résultats du module amont est disponible.

WO 01/17159 A1

WO 01/17159 A1



En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

METHODE D'ENCRYPTAGE MULTI-MODULES

La présente invention concerne le domaine du chiffrement, ou encryptage, et du déchiffrement ou décryptage de données, et particulièrement de données devant rester inaccessibles aux personnes ou appareils non autorisés dans le cadre de systèmes de télévision à péage. Dans de tels systèmes, les données sont chiffrées dans un environnement sécurisé, abritant des puissances de calcul importantes, et appelé sous-système d'encodage, puis envoyées, par des moyens connus en soi, vers au moins un sous-système décentralisé où elles sont déchiffrées, généralement au moyen d'un IRD (Integrated Receiver Decoder) et avec l'aide d'une carte à puce. Cette carte à puce et le sous-système décentralisé qui coopère avec elle sont librement accessibles par une personne éventuellement non autorisée.

Il est connu de chaîner divers moyens d'encryptage-décryptage dans un système de chiffrement-déchiffrement. Dans toute la suite, on appellera encryptage - décryptage un moyen de cryptage particulier utilisé dans un système plus vaste de chiffrement-déchiffrement.

On cherche depuis longtemps à optimiser le fonctionnement de ces systèmes du triple point de vue de la rapidité, de la place occupée en mémoire et de la sécurité. La rapidité s'entend au sens du temps nécessaire pour déchiffrer les données reçues.

Il est connu des systèmes d'encryptage - décryptage à clés symétriques. Leur sécurité inhérente peut être qualifiée en fonction de plusieurs critères.

Le premier critère est celui de la sécurité physique, relative à la facilité ou à la difficulté d'une méthode d'investigation par extraction de certains composants, suivie de leur remplacement éventuel par d'autres composants. Ces composants de remplacement, destinés à renseigner la personne non autorisée sur la nature et le fonctionnement du système de chiffrement-déchiffrement, sont choisis par elle de manière à ne pas être détectés, ou le moins possible, par le reste du système.

Un second critère est celui de la sécurité système, dans le cadre de laquelle les attaques ne sont pas intrusives du point de vue physique mais font appel à de l'analyse de type mathématique. Typiquement, ces attaques seront menées par des ordinateurs de grande puissance qui tenteront de casser les algorithmes et les codes de chiffrement.

Des moyens d'encryptage - décryptage à clés symétriques sont par exemple les systèmes appelés DES (Data Encryption Standard). Ces moyens, relativement anciens, n'offrent plus qu'une sécurité système et une sécurité physique toute relatives. C'est notamment pour cette raison que de plus en plus, le DES, dont les longueurs de clés sont trop petites pour satisfaire aux conditions de sécurité système, est remplacé par des moyens d'encryptage - décryptage nouveaux ou avec des clés plus longues. De manière générale, ces moyens à clés symétriques font appel à des algorithmes comprenant des rondes de chiffrement.

D'autres stratégies d'attaques sont appelées Simple Power Analysis, et Timing Analysis. Dans le Simple Power Analysis, on utilise le fait qu'un microprocesseur chargé d'encrypter ou de décrypter des données est connecté à une source de tension (en général 5 Volts). Lorsqu'il est au repos, il est parcouru par un courant fixe d'intensité i . Quand il est actif, l'intensité instantanée i est fonction, non seulement des données entrantes, mais aussi de l'algorithme d'encryptage. Le Simple Power Analysis consiste à mesurer le courant i en fonction du temps. On peut de ce fait déduire le type d'algorithme que le microprocesseur effectue.

De la même manière, la méthode du Timing Analysis consiste à mesurer la durée de calcul en fonction d'un échantillon présenté au module de décryptage. Ainsi, la relation entre l'échantillon présenté et le temps de calcul du résultat permet de retrouver les paramètres secrets de module de décryptage tel que la clé. Un tel système est décrit par exemple dans le document "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems" publié par Paul Kocher, Cryptography Research, 870 Market St, Suite 1088, San Francisco, CA-USA.

Pour améliorer la sécurité du système de chiffrement, il a été proposé des algorithmes à clé asymétriques, tels que les systèmes dits RSA (Rivest, Shamir et Adleman). Ces systèmes comprennent la génération d'une paire de clés appariées, l'une dite publique servant au chiffrement, et l'autre dite privée servant au déchiffrement. Ces algorithmes présentent un haut niveau de sécurité tant système que physique. Ils sont par contre plus lents que les systèmes traditionnels, surtout au stade du chiffrement.

Les techniques d'attaque les plus récentes font appel à la notion dite DPA, de l'anglais Differential Power Analysis. Ces méthodes sont basées sur des supputations, vérifiables au bout d'un grand nombre d'essais, sur la présence d'un 0 ou d'un 1 dans une position donnée de la clé de chiffrement. Elles sont quasiment non destructives, ce qui leur confère une bonne indétectabilité, et font appel à la fois à une composante d'intrusion physique et à une composante d'analyse mathématique. Leur fonctionnement rappelle les techniques d'investigation de champs pétrolifères, où une explosion de puissance connue est générée en surface et où des écouteurs et sondes, placés à des distances également connues du lieu de l'explosion, permettent d'émettre des suppositions sur la composition stratigraphique du sous-sol sans trop avoir à le creuser, grâce à la réflexion des ondes de choc par les limites de couches sédimentaires dans ce sous-sol. Les attaques DPA sont décrites notamment dans le § 2.1. du document "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards", publié le 1er février 1999 par Suresh Chari, Charanjit Jutla, Josyula R. Rao et Pankaj Rohatgi, de l'IBM T.J. Watson Research Center, Yorktown Heights, NY.

L'exigence de devoir résister aux attaques DPA oblige à utiliser des systèmes de brouillage dit "whitening", soit dans les informations à l'entrée, soit en sortie d'un algorithme de chiffrement-déchiffrement. La technique du whitening est décrite dans le § 3.5 du même document précité.

De plus le fait que les puissances de calcul soient limitées dans le sous-système décentralisé d'un système de télévision à péage crée un problème, qui n'a jamais encore été résolu de façon satisfaisante, pour effectuer dans une mesure suffisante le chaînage décrit précédemment.

Le but de la présente invention est de disposer d'une méthode d'encryptage-décryptage qui résiste aux méthodes modernes d'investigation telles que décrites ci-dessus.

5 Le but visé par la présente invention est atteint par la méthode décrite dans la partie caractérisante de la revendication 1.

La particularité de la méthode réside dans le fait qu'un module intermédiaire ne démarre pas lorsque le résultat du module précédent (ou amont) a terminé mais débute dès qu'une partie déjà des informations sont disponibles. De ce fait, pour un observateur extérieur, il n'est pas possible d'établir les conditions
10 d'entrée ou de sortie de ce module.

Comme le déchiffrement intervient dans le sous-système décentralisé coopérant avec la carte à puce, cette carte à puce n'abritant que des puissances de calcul relativement limitées par rapport au sous-système d'encodage, il est par exemple intéressant d'utiliser une clé asymétrique publique, au
15 fonctionnement relativement rapide, lors des dernières étapes du déchiffrement. Ceci permet d'une part de préserver les caractéristiques d'invulnérabilité du système en sortie de processus, et d'autre part de concentrer la puissance de calcul, liée essentiellement au chiffrement à l'aide de la clé privée, dans le sous-système d'encodage.

20 Il a été découvert qu'une sécurité supplémentaire est procurée par la possibilité de concaténer, ou d'imbriquer partiellement, deux moyens d'encryptage-décryptage qui se suivent séquentiellement. On entend par cette concaténation ou imbrication partielle, qui est une traduction de l'anglais "interleaving", le procédé consistant à démarrer l'action du deuxième moyen
25 d'encryptage-décryptage sur les données à un moment où le premier moyen d'encryptage-décryptage n'a pas encore terminé son travail sur ces mêmes données. Ceci permet de masquer les données telles qu'elles résulteraient du travail du premier module et avant qu'elles ne soient soumises à l'action du deuxième module.

La chaînage peut démarrer dès que des données calculées en sortie du premier module sont partiellement disponibles pour être traitées par le second module.

- 5 L'invention permet de se prémunir contre les attaques précitées en combinant divers moyens d'encryptage-décryptage dans un système de chiffrage-déchiffage, et en associant éventuellement une concaténation ou imbrication partielle à la séquence dans laquelle se suivent ces moyens.

10 Dans une forme particulière de réalisation de l'invention, le système de chiffrage-déchiffage comprend un sous-système d'encodage où trois algorithmes sont utilisés séquentiellement:

- a) un algorithme A1 asymétrique à clé privée d1. Cet algorithme A1 effectue une signature sur des données en clair, représentées par un message m, cette opération délivrant un premier cryptogramme c1, au moyen d'opérations mathématiques généralement notées dans la profession par la
- 15 formule : $c1 = m \text{ exposant } d1, \text{ modulo } n1$. Dans cette formule, n1 fait partie de la clé publique de l'algorithme asymétrique A1, modulo représente l'opérateur mathématique bien connu des congruences dans l'ensemble des entiers relatifs, et d1 est la clé privée de l'algorithme A.
- b) un algorithme S symétrique utilisant une clé secrète K. Cet algorithme
- 20 convertit le cryptogramme c1 en un cryptogramme c2.
- c) un algorithme A2 asymétrique à clé privée d2. Cet algorithme A2 convertit le cryptogramme c2 en un cryptogramme c3, au moyen de l'opération mathématique notée, comme précédemment, par : $c3 = c2 \text{ exposant } d2 \text{ mod } n2$, formule dans laquelle n2 fait partie de la clé publique de
- 25 l'algorithme asymétrique A2, et d2 est la clé privée de l'algorithme A2

Le cryptogramme c3 part du sous-système d'encodage et parvient au sous-système décentralisé par des moyens connus en soi. Dans le cas de systèmes de télévision à péage, il peut s'agir aussi bien de données vidéo que de messages.

Le sous-système décentralisé utilise, dans l'ordre inverse du précédent, trois algorithmes $A1'$, S' et $A2'$. Ces trois algorithmes font partie de trois moyens de cryptage-décryptage $A1-A1'$, $S-S'$ et $A2-A2'$, répartis entre le sous-système d'encodage et le sous-système décentralisé, et représentant le système de

5 chiffrement-déchiffrement.

d) l'algorithme $A2'$ effectuée sur $c3$ une opération mathématique restituant $c2$ et notée: $c2 = c3$ exposant $e2$ mod $n2$. Dans cette formule, l'ensemble constitué de $e2$ et $n2$ est la clé publique de l'algorithme asymétrique $A2-A2'$.

e) l'algorithme symétrique S' symétrique utilisant la clé secrète K restitue

10 le cryptogramme $c1$.

f) l'algorithme $A1'$ asymétrique à clé publique $e1$, $n1$ retrouve m en effectuant l'opération mathématique notée: $m = c1$ exposant $e1$ mod $n1$.

La concaténation, dans le sous-système décentralisé, consiste à démarrer l'étape de décodage e) alors que $c2$ n'a pas encore été totalement restitué par

15 l'étape précédente d), et à démarrer l'étape de décodage f) alors que $c1$ n'a pas été totalement restitué par l'étape e. L'avantage est de déjouer une attaque qui viserait par exemple d'abord à extraire, dans le sous-système décentralisé, le cryptogramme $c1$ en fin d'étape e, pour le comparer avec les données en clair m , puis au moyen de $c1$ et de m d'attaquer l'algorithme $A1'$,

20 puis de remonter la chaîne de codage de proche en proche.

La concaténation n'est pas nécessaire dans le sous-système d'encodage, qui est installé dans un environnement physique sécurisé. Elle est par contre utile dans le sous-système décentralisé. Dans le cas de la télévision à péage, l'IRD est en effet installé chez l'abonné et peut être l'objet des attaques du type

25 prédéfini.

On conçoit qu'une attaque d'une combinaison de trois algorithmes de décryptage $A1'$, S' et $A2'$ concaténés a beaucoup moins de chances de réussir que si les cryptogrammes $c1$ et $c2$ sont intégralement reconstitués entre chaque étape d), e) et f). Par ailleurs, le fait que les algorithmes $A1'$ et

30 $A2'$ soient utilisés avec des clés publiques $e1$, $n1$ et $e2$, $n2$ fait que les

moyens de calcul nécessaires dans le sous-système décentralisé sont bien plus réduits que dans le sous-système d'encodage.

A titre d'exemple et pour fixer les idées, les étapes a) et c) c'est-à-dire les étapes d'encryptage avec clés privées, sont 20 fois plus longues que les
5 étapes d) et f) de décryptage avec clés publiques.

Dans une forme particulière de réalisation de l'invention, dérivée de la précédente, les algorithmes A1 et A2 sont identiques de même que leurs contreparties A1' et A2'.

Dans une forme particulière de réalisation de l'invention, également dérivée
10 de la précédente, dans l'étape c) on utilise la clé publique e2, n2 de l'algorithme asymétrique A2 alors que dans l'étape d) on décrypte le cryptogramme c3 avec la clé privée d2 de cet algorithme. Cette forme constitue une alternative possible lorsque les ressources du sous-système décentralisé en puissance de calcul sont loin d'être atteintes.

15 Bien que les cartes à puces sont utilisées majoritairement pour le décryptage des données, il existe également des cartes à puces ayant les capacités nécessaires pour effectuer des opérations de cryptage. Dans ce cas, les attaques décrites plus haut vont se porter également sur ces cartes de cryptage qui fonctionnent hors d'endroits protégés tels qu'un centre de
20 gestion. C'est pourquoi la méthode selon l'invention s'applique également aux opérations de cryptage en série c'est à dire que le module aval débute son opération de cryptage dès qu'une partie des informations délivrées par le module amont sont disponibles. Ce procédé a l'avantage d'imbriquer les différents modules de cryptage avec comme conséquence que le résultat du
25 module amont n'est pas disponible complètement à un temps donné. De plus, le module en aval ne débute pas ses opérations avec un résultat complet mais sur des parties ce qui rend impraticable d'interpréter le fonctionnement d'un module par rapport à un état d'entrée ou de sortie connu.

La présente invention sera comprise plus en détail grâce aux dessins
30 suivants, pris à titre non limitatifs, dans lesquels:

- la figure 1 représente les opérations de cryptage
- la figure 2 représente les opérations de décryptage
- la figure 3 représente une alternative à la méthode de cryptage

Sur la figure 1, un ensemble de données m est introduit dans la chaîne de cryptage. Un premier élément $A1$ effectue une opération de cryptage en utilisant la clé dite privée composée de l'exposant $d1$ et du modulo $n1$. Le résultat de cette opération est représenté par $C1$. Selon le mode de fonctionnement de l'invention, dès qu'une partie du résultat $C1$ est disponible, le module suivant débute son opération. Ce module suivant S effectue son opération de cryptage avec une clé secrète. Le résultat $C2$ dès que partiellement disponible est transmis au module $A2$ pour la troisième opération de cryptage utilisant la clé dite privée composée de l'exposant $d2$ et du modulo $n2$. Le résultat final, dénommé ici $C3$ est prêt pour être transmis par des voies connues tels que voie hertzienne ou par câble.

La figure 2 représente le système de décryptage composé des trois modules de décryptage $A1'$, S' , $A2'$ similaires à ceux ayant servi à l'encryptage, mais ordonné inversement. Ainsi, l'on commence d'abord avec le module $A2'$ qui effectue son opération de décryptage sur la base de la clé dite publique composées de l'exposant $e2$ et du modulo $n2$. De la même manière que pour l'encryptage, dès qu'une partie du résultat $C2$ du module $A2'$ est disponible, il est transmis au module S' pour la deuxième opération de décryptage. Pour terminer le décryptage, le module $A1'$ effectue son opération sur la base de la clé dite publique composée de l'exposant $e1$ et du modulo $n1$.

Dans une forme particulière de l'invention, les clés des deux modules $A1$ et $A2$ sont identiques, c'est-à-dire que côté encryptage, $d1=d2$ et $n1=n2$. Par analogie, lors du décryptage, $e1=e2$ et $n1=n2$. Dans ce cas, on parle de la clé privée d , n et de la clé publique e , n .

Dans une autre forme de l'invention, telle qu'illustrée aux figures 3 et 4, le module $A2$ utilise la clé dite publique à la place de la clé dite privée. Au moment de l'encryptage, la clé publique $e2$, $n2$ est utilisée par le module $A2$,

(voir figure 3) et lors du décryptage (voir figure 4), le module A2' utilise la clé privée d_2 , n_2 pour opérer. Bien que cette configuration présente une surcharge de travail à l'ensemble de décryptage, l'utilisation d'une clé privée renforce la sécurité offerte par le module A2.

- 5 L'exemple illustré aux figures 3 et 4 n'est pas restrictif pour d'autres combinaisons. Par exemple, il est possible de configurer le module A1 pour qu'il effectue l'opération d'encryptage avec la clé publique et le décryptage avec la clé privée.

- 10 Il est également possible de remplacer le module d'encryptage-décryptage à clé secrète S par un module de type à clé asymétriques du même type que les module A1 et A2.

REVENDICATIONS

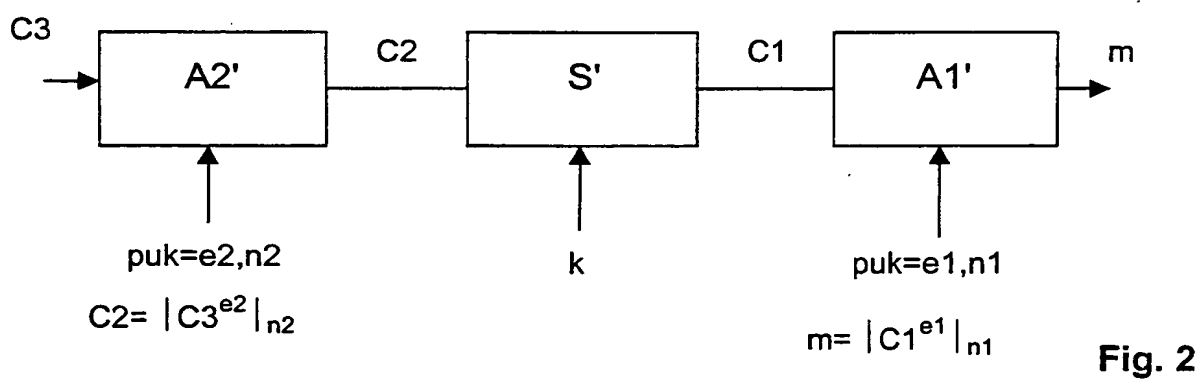
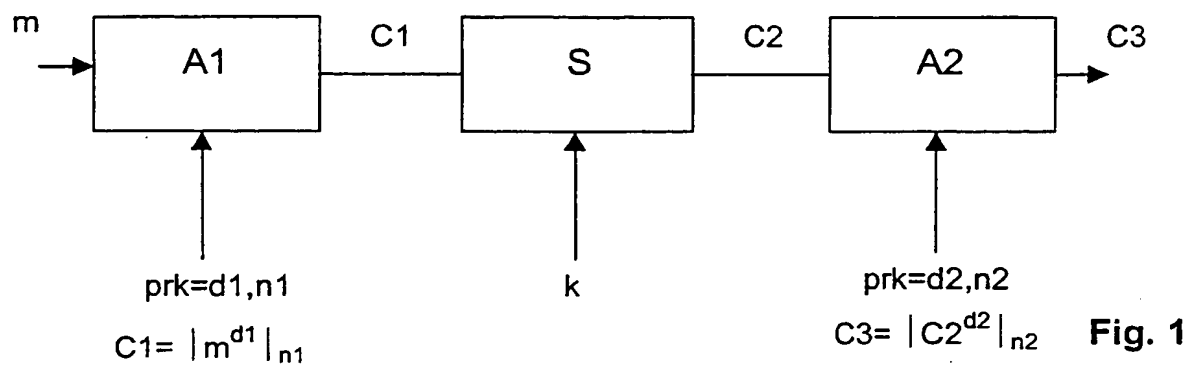
1. Méthode de cryptage et de décryptage utilisant plusieurs modules d'encryptage-décryptage en série, caractérisée en ce que le module d'encryptage-décryptage en aval débute son opération dès qu'une partie du résultat du module d'encryptage-décryptage amont est disponible.
2. Méthode selon la revendication 1, caractérisée en ce que le module de décryptage en aval débute son opération de décryptage dès qu'une partie du résultat du module de décryptage amont est disponible.
3. Méthode selon la revendication 1, caractérisée en ce que le module d'encryptage en aval débute son opération de cryptage dès qu'une partie du résultat du module amont est disponible.
4. Méthode selon les revendication 1 à 3, caractérisée en ce qu'elle met en œuvre trois modules (A1, S, A2), le module central (S) étant de type à clé symétrique secrète (k).
5. Méthode selon la revendication précédente, caractérisée en ce que le premier module (A1) et le dernier module (A2) pour l'encryptage et le premier module (A2) et le dernier module (A1) pour le décryptage sont du type RSA à clés asymétriques soit avec une clé privée et une clé publique.
6. Méthode selon la revendication précédente, caractérisée en ce que les deux modules (A1, A2) utilisent la clé dite privée (d, n ; d_1, n_1 ; d_2, n_2) pour l'encryptage et la clé dite publique (e, n ; e_1, n_1 ; e_2, n_2) pour le décryptage.
7. Méthode selon la revendication précédente, caractérisée en ce que les deux modules (A1, A2) utilisent un même jeu de clé privée (d, n) et publique (e, n).

8. Méthode selon la revendication 6, caractérisée en ce que les deux modules (A1, A2) utilisent un jeu différent de clés privée ($d1, n1$; $d2, n2$) et publique ($e1, n1$; $e2, n2$).

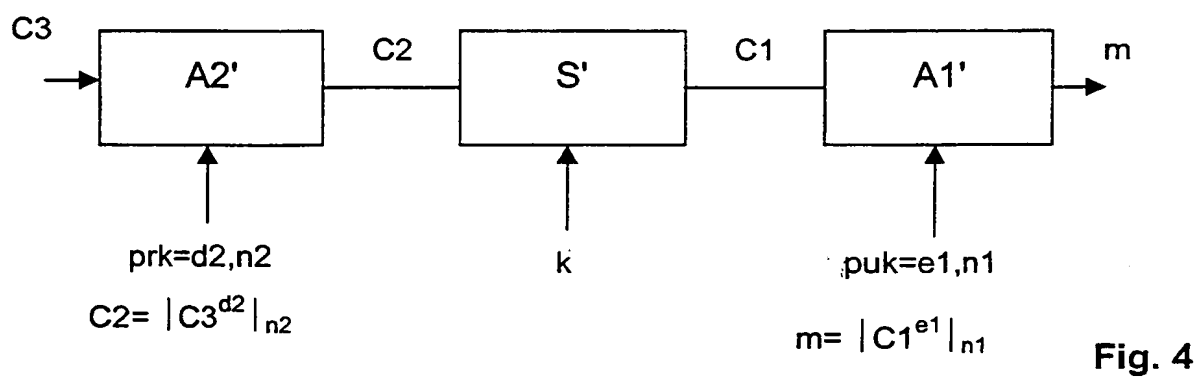
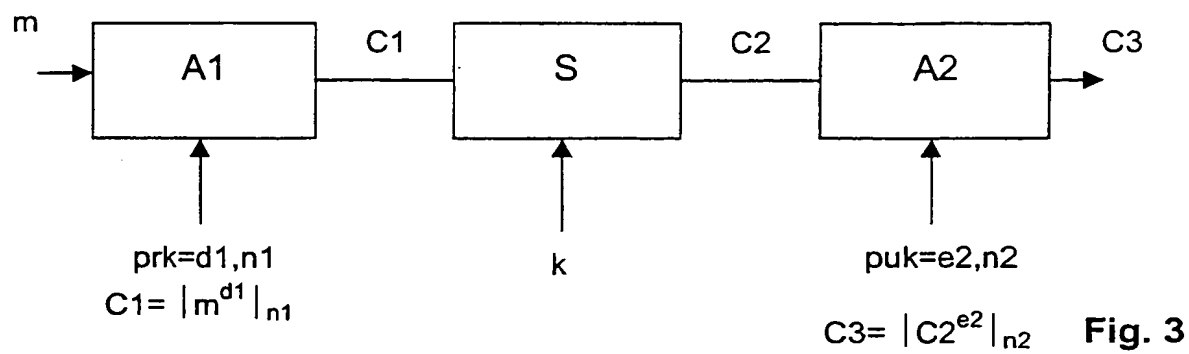
9. Méthode selon la revendication 5, caractérisée en ce que lors de l'encryptage, le dernier module (A2) utilise la clé dite publique ($e2, n2$) et lors du décryptage, le premier module (A2) utilise la clé dite privée ($d2, n2$).

10. Méthode selon les revendications 1 à 3, caractérisée en ce qu'elle met en œuvre trois modules (A1, A, A2) d'encryptage-décryptage à clés asymétriques.

This Page Blank (uspto)



This Page Blank (uspto)



This Page Blank (uspto)

INTERNATIONAL SEARCH REPORT

International Application No

PCT/IB 00/01157

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 594 797 A (ALANAERAE SEPP0 ET AL) 14 January 1997 (1997-01-14) abstract column 2, line 5 - line 32 column 7, line 59 -column 8, line 13 claim 1 figure 3	1-10
A	DE 195 39 700 C (SIEMENS AG) 28 November 1996 (1996-11-28) abstract column 3, line 30 -column 4, line 18 claim 1 figure 1	1-10
	-/-	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

15 November 2000

Date of mailing of the international search report

22/11/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Holper, G

INTERNATIONAL SEARCH REPORT

International Application No

PCT/IB 00/01157

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>RENZY M ET AL: "A BLOCK CIPHER METHOD USING COMBINATIONS OF DIFFERENT METHODS UNDER THE CONTROL OF THE USER KEY" PROCEEDINGS OF THE WORKSHOP ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES, DE, BERLIN, SPRINGER, vol. CONF. 3, page 531-534 XP000470470 ISBN: 3-540-57220-1 the whole document</p>	1-6, 9, 10

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. Application No

PCT/IB 00/01157

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5594797	A	14-01-1997	BR 9600772 A	23-12-1997
			CA 2168717 A	23-08-1996
			CN 1136738 A	27-11-1996
DE 19539700	C	28-11-1996	WO 9716003 A	01-05-1997
			EP 0857382 A	12-08-1998
			JP 11513864 T	24-11-1999

This Page Blank (uspto)

RAPPORT DE RECHERCHE INTERNATIONALE

Der Internationale No

PCT/IB 00/01157

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

CIB 7 H04L9/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 5 594 797 A (ALANAERAE SEPPO ET AL) 14 janvier 1997 (1997-01-14) abrégé colonne 2, ligne 5 - ligne 32 colonne 7, ligne 59 - colonne 8, ligne 13 revendication 1 figure 3	1-10
A	DE 195 39 700 C (SIEMENS AG) 28 novembre 1996 (1996-11-28) abrégé colonne 3, ligne 30 - colonne 4, ligne 18 revendication 1 figure 1	1-10
	-/-	

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"Z" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

15 novembre 2000

Date d'expédition du présent rapport de recherche internationale

22/11/2000

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Holper, G

RAPPORT DE RECHERCHE INTERNATIONALE

Document International No

PCT/IB 00/01157

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>RENZY M ET AL: "A BLOCK CIPHER METHOD USING COMBINATIONS OF DIFFERENT METHODS UNDER THE CONTROL OF THE USER KEY" PROCEEDINGS OF THE WORKSHOP ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES, DE, BERLIN, SPRINGER, vol. CONF. 3, page 531-534 XP000470470 ISBN: 3-540-57220-1 le document en entier</p>	1-6,9,10

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Der. Internationale No

PCT/IB 00/01157

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5594797 A	14-01-1997	BR 9600772 A	23-12-1997
		CA 2168717 A	23-08-1996
		CN 1136738 A	27-11-1996
DE 19539700 C	28-11-1996	WO 9716003 A	01-05-1997
		EP 0857382 A	12-08-1998
		JP 11513864 T	24-11-1999

This Page Blank (uspto)